

Building a More Effective Strategy for ICT Supply Chain Security

Executive Summary

The Biden Administration and the 117th Congress should take a new, more effective approach to Information and Communications Technology (ICT) supply chain security. That process should begin by pausing and assessing the inventory of US supply chain security rules to move forward more effectively with a holistic and sustainable set of policies to improve security.

There are significant supply chain security threats from both government and non-governmental actors. In response to recent foreign government intrusions into US networks, the Biden Administration proposed significant investment in the Technology Modernization Fund to begin the hard work of moving toward a more secure digital ecosystem.

Global ICT supply chains continue to be important for the digital economy, but we need a modernized approach to supply chain security. In recent years, unfortunately, the government's actions have lacked a strategic focus and the articulated rationales for actions have been muddled—often conflating economic and national security objectives. Current policies are primarily based on intervention or country-based limitations. These policies are largely reactive, and they are often overly broad to the point where they become counterproductive to both security and economic growth.

In this white paper, BSA calls for a shift in emphasis to an assurance-based approach, coordinated across government agencies with a strategic focus. Assurance policies create incentives for companies to adopt best practices and improve the technology used to protect the supply chain. They are focused on risk-management that is more nuanced and tailored to the current environment, and more agile to adapt to future threats, than interventionist approaches.

The US government should reassert itself as a leader on security issues, working in both formal and informal alliances to improve collaboration with like-minded countries and create the global approach needed for success. Public-private partnerships, which, among other things, can create high-level standards and norms, is an important part of this approach.

BSA calls for a shift in emphasis to an assurance-based approach, coordinated across government agencies with a strategic focus.

Background

The US information technology (IT) industry faces real and significant threats to its supply chains. Supply chains are complex, global, and the target of malicious actors who have varying degrees of sophistication and different objectives. The threats can come from amateur hackers, disgruntled employees, criminal networks, and sophisticated nation-state actors. Each can present a risk to the integrity and security of supply chains for hardware, software, and related products and services. As both the economy and security of the United States have become increasingly dependent on IT, confronting these threats has become ever more important.

Supply chain threats can target hardware components, such as an Internet of Things (IoT) device, or software components, such as the operating system. The intrusion can happen at any point in the supply chain, with or without the knowledge of a supplier. And it can be introduced when data storage and processing are done on premises or in a cloud environment, despite the additional available security protections. This makes vetting and oversight of third-party vendors particularly important.

The US government has rightly prioritized supply chain risk management. In recent years, the government's efforts have largely focused on threats posed by either direct or indirect nation-state actors. Nation-state actors pose a **direct** threat to US supply chains when they maliciously intervene to compromise products and services relying on those supply chains. The recent revelation that SolarWinds's Orion network monitoring software had been compromised to gain illicit access to at least 18,000 sensitive government and private networks—an intrusion attributed by the US Intelligence Community to the Russian government—is a paradigmatic *direct* threat: the nation-state specifically intervened in a trusted process to gain access to networks used by businesses and another government's agencies.

The US government has also increasingly been concerned about **indirect** threats posed by nation-state actors. Nation-states may pose an *indirect* threat when an organization outside the government—a company, for example—is controlled by that government and establishes a position in the international marketplace that *could* enable it to threaten US interests. Huawei has been asserted by the US government to present such a threat; it occupies a major share of the 5G market, particularly for Radio Access Network (RAN) technology. US officials are concerned that Huawei, which has deep ties to the Chinese military and Communist Party and is required by Chinese law to assist in national security matters, could exploit that position to compromise or disrupt large volumes of data passing through 5G networks.

The US government has approached both direct and indirect threats to the supply chain using tools that can generally be grouped into three categories:

- 1 Intervention.**
Policies in this category enable the government to intervene in specific business transactions determined to represent a threat to US supply chains to modify, disrupt, or prohibit those transactions. Intervention policies are generally reactive in nature.
- 2 Country-Based Limitations.**
Some policies prohibit or limit certain business activities through a country-specific application of rules; for example, limiting business operations within a certain country, or limiting certain business transactions with an entity based in a certain country.
- 3 Assurance.**
Assurance-based policies establish incentives or requirements to encourage organizations to meet supply chain risk management, transparency, and integrity benchmarks, generally based on widely recognized technical standards.

Each of these policy approaches carry advantages and disadvantages, which will be discussed further in the following section. In general, over the last four years, US policy has been too focused on intervention and country-based limitations. Although these approaches include important tools, a shift toward sustainable, assurance-based measures will improve the overall state of US security and global supply chain management.¹

Challenges in Current Policies Focused Primarily on Intervention and Country-Based Limitations

The previous Administration adopted numerous policies to address supply chain risks, both by initiating executive actions and implementing legislation. Table 1 summarizes major supply chain policies adopted under the Trump Administration. As the table demonstrates, the previous Administration has relied heavily on intervention and country-based limitation policies, with limited emphasis on assurance. This overly blunt approach has been challenging or impractical to implement, harmful and confusing to US industry, and all without ultimately advancing any real supply chain security.

Table 1. Supply Chain Policies Adopted Under the Previous Administration

POLICY	SUMMARY	POLICY TYPE
Executive Actions		
Executive Order 13873	Authorizes government intervention in any business transaction with an entity in an adversarial country deemed to be a threat.	Intervention, Country-Based Limitation
Executive Order 13942	Prohibits transactions with Chinese company Tik-Tok.	Country-Based Limitation
Executive Order 13943	Prohibits transactions with Chinese company WeChat.	Country-Based Limitation
Executive Order 13971	Prohibits transactions with several Chinese companies, including Tencent QQ and Alipay.	Country-Based Limitation
Executive Order 13984, amending Executive Order 13694	Authorizes restrictions or prohibitions on customers of Internet as a Service providers.	Intervention, Country-Based Limitation
Bureau of Industry and Security Entity List Designations	Prohibits transactions with specified companies based on national security interests.	Intervention, Country-Based Limitation
Cybersecurity Maturity Model Certification (CMMC)	Requires DoD vendors to obtain information security certifications based on CMMC framework.	Assurance

¹ The recommendation to focus on assurance-based policies is consistent with the recommendations recently released by the Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain," CSC White Paper #4 (October 2020), available at <https://www.solarium.gov/public-communications/supply-chain-white-paper>.

POLICY	SUMMARY	POLICY TYPE
Legislative Actions		
Sec. 889, Fiscal Year 2019 National Defense Authorization Act (FY 2019 NDAA)	Prohibits federal acquisition from vendors who use technology or services provided by Chinese-based companies including Huawei and ZTE.	Country-Based Limitation
Sec. 1655, FY 2019 NDAA	Requires disclosure when companies allow foreign governments to conduct reviews of their source code.	Intervention, Country-Based Limitation
<i>Federal Acquisition Supply Chain Security Act</i>	Authorizes the federal government to intervene in acquisitions to remove or exclude vendors determined to pose risk.	Intervention
Sec. 841, FY 2021 NDAA	Prohibits acquisition of printed circuit boards from various countries.	Country-Based Limitation


The government has been challenged to implement many of these interventionist and country-based policies because of their breadth and the bluntness of the approach. For many of the Executive Orders, the Trump Administration was unable to reach agreement on implementing rules. The Executive Orders were written so broadly that they would require capacity that responsible US government agencies recognized they do not have. And their unintended consequences would be far reaching. For example:

- » The supply chain Executive Order (EO 13873) would require the Department of Commerce to monitor every business transaction involving ICT products from China—the United States’ second-largest trading partner—to identify and intervene in risky transactions, a task that would overwhelm the Department if fully executed.
- » Section 889 of the FY 2019 NDAA is intended to prohibit the federal government from contracting with any business that uses a technology with Huawei- or ZTE-produced components anywhere in the world. A multinational company could be excluded if it uses broadband internet services in one of the many countries in the world where Huawei provides technologies for internet infrastructure, such as the United Kingdom or Germany. In fact, in many cases, it may be impossible for a business to know anything about what sorts of technology its internet provider uses for its internal infrastructure. Such a provision could easily exclude most US-based multinational businesses.

The broad scope of these policies has not just made them impractical to implement; it has also created serious challenges for the US technology industry. First, as the Section 889 example above illustrates, it has created compliance obligations nearly impossible to meet and that are costly for both government and industry, and it creates a deeply uncertain regulatory environment for key parts of US industry.

Second, the broad and country-focused approach of many supply chain policies has been coupled with incoherent and unclear explanations of the threats that these policies are intended to address—often conflating national security and economic protectionism. The undisciplined messaging has exacerbated perceptions that the US has used national security authorities in pursuit of economic objectives, undermining the credibility of these policies and inviting greater economic protectionism abroad. The result has been to undermine the global competitiveness of the very US businesses that are needed to protect supply chains.

These challenges are the inevitable result of relying too heavily on overly broad intervention- and country-based approaches to supply chain security. Intervention-based approaches can create an untenable burden on government agencies to pick out potentially risky activities from among the millions of business



Assurance policies can incent strong security practices across the supply chain, reducing risk widely instead of depending on targeted interventions.

transactions occurring across the US economy each year—they require searching for needles in haystacks. Meanwhile, country-based limitations face a substantial burden to demonstrate that they are not unfairly targeting competitors for economic reasons, and they carry a high risk of sparking retaliatory action by targeted countries. Neither of these outcomes serves either government or industry interests.

The previous Administration's policies represent a suboptimal solution to a clear and concerning challenge; they have created confusion and incoherence in government implementation, while leaving US industry to face regulatory uncertainty, new challenges to overseas competitiveness, and obstacles to sustained innovation. And they have not enhanced security in any targeted or meaningful way. As the Biden Administration and the new Congress begin, an urgent priority must be to set a new course on supply chain security.

The Way Forward: Assurance-Based Supply Chain Security

A recalibrated approach to supply chain security should, first and foremost, undertake a major conceptual shift, from defaulting to policies of intervention and country-based limitation to an assurance-focused approach. Assurance policies can incent strong security practices across the supply chain, reducing risk widely instead of depending on targeted interventions. They build confidence in security and trust in vendors by establishing consistently applied criteria, rather than creating confusion and inviting retaliation. And they guide the market to compete based on security, driving security-focused innovation.²

GUIDING PRINCIPLES

In undertaking this conceptual shift, the Biden Administration and Congress should be guided by the following principles:³

- 1 Ensure policies are cohesive and holistic.** Policies affecting supply chain security should be consistent and coordinated across the US government. Policymakers should consider whether specific decisions are consistent with the overall strategic objective, including by identifying unintended consequences from any specific action, and ensuring that requirements are not duplicative across sectors and agencies.
- 2 Ensure policies are risk-based.** Risk management entails understanding risk by identifying likely threats, vulnerabilities, and potential consequences; tailoring mitigation strategies to risks; and prioritizing actions based on the most relevant and potentially impactful risks. Risk management approaches consider not only risks from malicious actors, but also the risks, timelines, and costs associated with potential mitigation options, helping policymakers avoid unintended consequences of mistargeted policies and achieve successful mitigation strategies.

² That is not to say that intervention and other policies have no place in supply chain risk management. It may be appropriate for the government to have the authority to intervene in specific transactions where there is a clearly articulable risk that assurance policies cannot address. Such policy tools should be deployed by exception, and in the context of an assurance-based policy environment that establishes consistent expectations for security.

³ For more detail on these principles, please see BSA's *Principles for Good Governance: Supply Chain Risk Management*, <https://www.bsa.org/files/policy-filings/07172019bsasupplychainprinciples.pdf>.

GUIDING PRINCIPLES *(continued)*

- 3 Ensure policies are narrowly tailored.** Policies should be targeted to address a specific security objective in the manner that is minimally disruptive to US interests, avoiding overbroad scoping that makes implementation impractical and ineffective.
- 4 Ensure policies will be acceptable when applied reciprocally.** Policies should consider the potential for sparking retaliatory action or constraining the ability of US industry to compete in overseas markets; policies should also avoid undermining innovation.
- 5 Ensure policies are transparent and offer clear routes to adjudicate adverse actions.** Uneven or non-transparent enforcement of supply chain policies calls into question their credibility and motive; policies should be consistently enforced. Moreover, when adverse decisions are made, impacted stakeholders should have a clear pathway to appeal or otherwise adjudicate the decisions.
- 6 Ensure policies are subject to robust public consultation and frequent review.** Understanding how a policy may impact US technological leadership and ensuring that policies will be effective against the threat they are intended to mitigate will necessitate open and candid dialogue with affected stakeholders, including industry. Ensuring that policies are developed and implemented in a transparent manner is also critical for guarding against false accusations that the US is using security as a pretext for advancing broader economic and trade ambitions.

Specific Recommendations

As the new Congress and the new Administration begin, policymakers should take immediate steps to implement a shift from intervention and country-based policies to assurance-driven supply chain risk management, in alignment with the principles articulated above. The following are recommendations for actions in the near- and medium-term to establish a supply chain security policy environment that is strong, effective, and respected globally.


Focus on Assurance

Government and industry, working together, will be far more effective in confronting supply chain threats than uncoordinated and sporadic intervention in individual transactions. Congress and the Biden Administration should:

Adopt Assurance Incentives

Policymakers should invest in maturing supply chain risk management attestation and, where appropriate, certification models, building on existing government efforts. The Department of Homeland Security (DHS) Supply Chain Risk Management Task Force has initiated work to develop a supply chain self-attestation methodology and to improve guidance for establishing Qualified Bidders Lists and Qualified Manufacturers Lists. That work should continue. Tools like security self-attestations and qualified lists can not only improve assurance in technologies acquired by the government, but also set expectations for security throughout the broader marketplace.

Additional efforts, such as Software Bill of Materials (SBOM) guidance developed by the National Telecommunications and Information Administration (NTIA), the Secure Software Development Framework (SSDF) developed by the National Institute of Standards and Technology (NIST), and BSA's own *Framework for Secure Software*, can be powerful when used as the basis for self-attestation or to inform qualified lists,



The US government should increase its investment in research and development around innovative technological solutions to supply chain risks.

and can provide incentives for stronger security practices. Demonstrating practices that are consistent with these frameworks can be useful for communicating to customers the standard of care used in software development. Frameworks and best practice guidance for those using and implementing IT services, such as guidance provided by NIST, are similarly important.

Some existing efforts, such as NIST's efforts to develop an IoT device security baseline, should also be continued, particularly to the extent they can improve clarity in underlying criteria and risk analysis. Broadly, there are substantial opportunities to encourage assurance in 5G technologies in ways likely to achieve desired results more effectively than intervention or country-based limitations. Other assurance efforts, such as the Defense Department's CMMC program, should be reconsidered because of their excessive implementation burden, which outweighs any security gains.

Invest in SCRM-Related Research and Development (R&D)

Many supply chain security challenges can be mitigated or eliminated by developing new technologies. Such technologies cover a wide range, including open RAN technologies to enhance competition and eliminate supplier dependence in 5G networks and solutions, new encryption technologies to better secure data at rest and in transit, software- and hardware-based supply chain integrity monitoring technologies, improved security of open source components, and new applications of blockchain concepts.

The US government should increase its investment in research and development around innovative technological solutions to supply chain risks, prioritizing research into critical dependencies in 5G supplier networks, cloud security, third-party software component risk management, and end-to-end supply chain integrity and transparency.

Strengthen the US Industrial Base to Ensure Access to Trusted Suppliers

Global supply chains are essential in order to enable multinational businesses to build resilience, source the best possible components, and remain agile. However, in some cases, supply chains would be strengthened through better availability of trusted US-based suppliers. The FY 2021 NDAA included legislation intended to spur domestic manufacturing capacity for semiconductors and other microelectronics; the US government should build on this effort to identify key technologies where insufficient trusted US-based suppliers exist and to invest in building a manufacturing base for such technologies.⁴ This should also be a consideration in any intervention-based decisions, which may weaken US industry's competitiveness over the long term and, as a result, create supply chain risks.


Strengthen US International Leadership on Supply Chain Risk Management

To extend the reach of assurance-based US supply chain policies, the US must exert global leadership to build active coalitions of likeminded partners. Congress and the Biden Administration should:

Forge Formal, Action-Oriented Partnerships to Address Common Supply Chain Challenges

The US and many of its key allies face similar concerns around technology supply chain risks, and many opportunities exist for unified action to confront these risks. Formal partnerships signal the commitment of groups of allies to tackle key challenges and maintain governance mechanisms to coordinate action. These partnerships can significantly affect the direction of internationally recognized technical standards or certifications, multilateral policy initiatives, and establishment and enforcement of global norms.

⁴ The Cyberspace Solarium Commission's "Building a Trusted ICT Supply Chain," *supra* at footnote 1, discusses this recommendation in detail.



➔ Policymakers should better resource government participation in international standards and norms development, and encourage broader participation of industry stakeholders.

Recalibrate Informal Partnerships to Strengthen Collaboration around Common Objectives

The US also works informally with allies and partners toward common goals. In recent years, however, the US approach has too often been to strongarm partners to adopt US positions or to neglect partner perspectives on potential policy solutions; as a result, informal collaboration has faltered. Efforts to persuade allies and partners to ban Huawei technologies offer an instructive example, leading some partners to take actions contrary to stated US goals. The new Administration must invest in recalibrating these informal efforts to build mutual trust and cooperation with key allies and partners, setting the foundation for more effective collaboration on common supply chain objectives.

Strengthen US Investment in International Standards Development and International Norms Development

Internationally recognized, industry-led technical standards form a critical basis for harmonizing global supply chain and cybersecurity policies and will shape the direction of key emerging technologies such as 5G network architectures. Likewise, international norms can constructively shape behavior of nation-state actors. In both environments, participation can be resource intensive, and too little has been invested in these processes. Policymakers should better resource government participation in standards and norms development, and encourage broader participation of industry stakeholders.

Invest in Foreign Partner Capacity-Building

Foreign partners can contribute to strengthening global supply chain integrity and security in numerous ways, from policing malicious activity within their own borders to sharing information and intelligence about identified risks. Modest investments in building the capacity of partners to adopt and implement smart supply chain policies can pay enormous dividends. Congress should work with the Biden Administration to authorize capacity-building initiatives in supply chain risk management and cybersecurity more broadly to build a robust capacity-building program.

Activate Public-Private Partnerships to Manage Supply Chain Risk

Government action will be most effective when it is buttressed by collaboration with key industry stakeholders that operate critical supply chains. Congress and the Biden Administration should:

Improve Supply Chain Threat Information-Sharing

Industry stakeholders operating across different sectors and in countries around the world will, collectively, see a far greater variety of supply chain risks, threats, and malicious actors than the US government will alone. Six years after the passage of the Cybersecurity Information Sharing Act, the government has yet to develop an agile, effective mechanism for the two-way sharing of threat information across a large swath of industry. Congress and the Biden Administration should work together with industry stakeholders, academics, and the public interest community, to identify the most relevant supply chain threat indicators and create an efficient mechanism for sharing such information.

Encourage Private Sector Leadership

Industry stakeholders have pioneered both technological and governance approaches to address supply chain risks, and the government should look to find creative ways to incent and harness these efforts. For example, in 2018, a coalition that now includes 17 major companies from around the world announced



the Charter of Trust, an initiative through which participants committed to enforce several supply chain risk management principles for themselves and their suppliers.⁵

That same year, more than 60 global companies signed onto the Cybersecurity Tech Accord,⁶ adopting several supply chain risk management commitments as part of a pledge to defend customers against cyber attacks. The government should develop incentives for such commitments, prioritizing relationships with companies that have taken demonstrable steps to mitigate supply chain risk.

Build Transparency and Formal Industry Participation Into Key Government Supply Chain Policy Processes

Government supply chain risk management policies are more likely to succeed when they consider the equities of impacted industry stakeholders. Multi-stakeholder processes such as those managed by NIST and NTIA have proven especially effective. Yet, some government supply chain processes—such as the Federal Acquisition Security Council (FASC)—remain opaque to industry. The Biden Administration should take measures to ensure transparency and provide a formal industry role in the FASC and similar processes.

Recalibrate Current Policies to Address Implementation Challenges

To kickstart the shift in policy outlined above, the challenges associated with existing policies created in the Trump Administration must be addressed. Congress and the Biden Administration should:

Narrow the Scope of Executive Order 13873 and Suspend Proposed Implementing Rules

Executive Order 13873 and accompanying implementing regulations should be overhauled to narrow authorities for intervention strictly to those transactions that pose a demonstrable, clearly articulated risk to US national security. The vagueness and broad scope of authority provided to the Department of Commerce in current draft regulations creates untenable challenges for the companies involved in supply chain security efforts and is impractical for the government to implement. A narrow authority, paired with broader emphasis on supply chain assurance, will retain a potentially useful tool for the government while strengthening the credibility, practicality, and certainty of the broader US approach to supply chain risk management.

Revisit Impractical Section 889 Requirements

Section 889's broad scope could potentially rule out any US multinational company from doing business with the US government, making it highly impractical and ultimately counterproductive. Congress and the Biden Administration should instead work together to refine Section 889 to limit the restrictions to those technologies that are actually intended for government use or acquisition, avoiding overbroad scope.

Change Course on CMMC

The Defense Department's CMMC has proven to be unworkable: administratively burdensome, overly bureaucratic, and compromised by conflicts of interest. The Department's objective of securing controlled, unclassified information throughout its supply chain is clearly important, but alternative approaches—more directly aligned with the existing NIST Special Publication 800-171—will be more likely to achieve this goal effectively and efficiently. The Department should pause implementation of CMMC while considering appropriate alternative policy mechanisms.

⁵ See www.charteroftrust.com.

⁶ See cybertechaccord.org.